CLAIMS

What is claimed is:

1. A security processing circuit for performing 3DES encryption or decryption services using a single DES engine, the security processing circuit comprising:

the single DES engine operable to provide security processing, the single DES engine employing an intermediate result at a data output of the single DES engine, to the single DES engine further comprising an input node adapted to selectively process input data from a data input of the security processing circuit during a first DES processing operation, and subsequently to process the intermediate result data from the data output during a second and third DES processing operation, respectively;

a select switch coupled to the data input of the security processing circuit, the data output, and the input node of the single DES engine, the select switch adapted to selectively couple one of the data input and the intermediate result to the input node of the single DES engine; and

a set of cipher keys selectively coupled to the single DES engine, wherein the security processing circuit is operable to select and load a different cipher key associated with each DES processing operation to the single DES engine during the three DES processing operations of the 3DES security processing.

2. The security processing circuit of claim 1, wherein the select switch is operable to selectively couple one of the data input and the intermediate result to the single DES engine according to the state of a selection signal coupled to the select switch.

3. The security processing circuit of claim 2, wherein the select switch comprises a multiplexor.

4. The security processing circuit of claim 1, wherein the set of cipher keys comprise three different cipher keys, each cipher key associated with one of the three DES processing operations of the 3DES security processing.

5. The security processing circuit of claim 4, further comprising a key select switch connected to inputs associated with the three cipher keys and a key data node of the single DES engine, the key select switch operable to selectively couple one of the three cipher keys associated with a DES processing operation to the single DES engine during the three DES processing operations of the 3DES security process.

6. The security processing circuit of claim 1, wherein the set of cipher keys selectively coupled to the single DES engine are selected and coupled using a multiplexor residing between the set of cipher keys and the single DES engine and wherein the set of cipher keys are connected to a set of multiplexor inputs and the single DES engine is connected to the multiplexor output.

7. The security processing circuit of claim 1, further comprising a clock input coupled to the single DES engine for timing clock cycles of the first, second and third DES processing operations of the 3DES processing for the security processing circuit.

8. The security processing circuit of claim 7, wherein the 3DES processing is completed in three single DES processing operations.

9. The security processing circuit of claim 7, wherein the 3DES processing is completed in eight clock cycles.

10. The security processing circuit of claim 7, wherein the first, second and third DES processing operations have a duration, wherein each comprises two clock cycles.

11. The security processing circuit of claim 9, wherein the clock cycle has a period of about 8ns.

12. The security processing circuit of claim 9, wherein the eight clock cycles of the 3DES security processing comprise:

a data input latch cycle;

a first DES processing operation comprising two cycles;

a second DES processing operation comprising two cycles;

a third DES processing operation comprising two cycles; and

a data output latch cycle.

13. The security processing circuit of claim 1, further comprising a segmentation system coupled with the security processing circuit, the segmentation system adapted to selectively segment outgoing data from the host system to create segment frames for transmission to a network.

14. The security processing circuit of claim 1, wherein the security processing circuit resides within a network interface device of a host system for performing 3DES encryption and decryption services for the host system using a single DES engine.

15. The security processing circuit of claim 1, further comprising a network interface device coupled with the security processing circuit, the network interface device being adapted to selectively encrypt outgoing data from a host system to cryptographically process data for transmission to a network.

16. The security processing circuit of claim 15, wherein the network interface device comprises a bus interface, a media access control system, and the security processing circuit.

17. The security processing circuit of claim 16, wherein the network interface device comprises a single integrated circuit.

18. The security processing circuit of claim 1, wherein the circuit comprises an IPsec circuit adapted to selectively provide authentication, encryption, and decryption functions for incoming and outgoing data.

19. A network interface device for interfacing a host system with a network to provide outgoing data from the host system to the network and to provide incoming data from the network to the host system, the network interface device comprising:

a bus interface coupled with a host bus in the host system, the bus interface being adapted to transfer data between the network interface device and the host system;

a media access control system coupled with the network, the media access control system being adapted to transfer data between the network interface device and the network; and

a security processing circuit coupled between the bus interface and the media access control system, the security processing circuit adapted to selectively encrypt outgoing data and to selectively decrypt incoming data, the security processing circuit comprising a single DES engine operable to perform 3DES processing of data by selectively feeding back intermediate data results to an input thereof to perform additional processing on the data.

20. The network interface device of claim 19, wherein the bus interface comprises a PCI-X bus interface coupled with a host PCI or PCI-X bus.

21. The network interface device of claim 19, wherein the media access control system comprises a MAC engine adapted to operate an Ethernet node and to provide an interface between the host system and the network.

22. The network interface device of claim 19, wherein the security processing circuit comprises an IPsec system adapted to selectively provide authentication, encryption, and decryption functions for incoming and outgoing data.

23. A method of 3DES processing security information from a host system to a network using a network interface device to 3DES process outgoing data from the host system to the network and to 3DES process incoming data from the network to the host system, the method comprising:

transferring data between the network interface device and the host system using a bus interface;

transferring data between the network interface device and the network using a media access control system;

obtaining security information from the host system, the security information being associated with outgoing data;

storing the outgoing data from the bus interface into a 3DES processing circuit;

selectively performing security processing on the outgoing data encrypting the data according to security key information and storing the outgoing data in the 3DES processing circuit using a single DES engine;

transferring the outgoing data from the 3DES processing circuit to the network interface device using the interface bus; and

transferring the outgoing data from the interface bus to the network using the media access control system.

24. The method of claim 23, wherein selectively performing the security processing on the outgoing data comprises selectively encrypting the outgoing data using the security processing circuit.

25. A method of performing 3DES encryption or decryption processing using a security processing circuit employing a single DES engine within a network interface device, the method comprising:

latching input data to a DataIn bus of the security processing circuit from the network interface device;

latching key data to a Key bus of the security processing circuit from the network interface device;

selecting and coupling the input data to an input data node of the single DES engine using a data select switch during a first DES processing operation;

selecting and coupling a first key from the key data to a key data node of the single DES engine using a key select switch during the first DES processing operation, the first key associated with the input data;

first DES processing the input data with the associated first key using the single DES engine of the security processing circuit;

obtaining a first intermediate result data from the first DES processing operation at a DataOut bus of the security processing circuit, the intermediate result being feedback coupled to a feedback input of the data select switch;

selecting and coupling the intermediate result data to the input data node of the single DES engine using the data select switch during a second DES processing operation;

selecting and coupling a second key from the key data to the key data node of the single DES engine using the key select switch during the second DES processing operation, the second key associated with the intermediate result data;

second DES processing the intermediate result data with the associated second key;

obtaining a second intermediate result from the second DES processing operation at the DataOut bus of the security processing circuit, the second intermediate result being feedback coupled to the feedback input of the data select switch;

selecting and coupling the second intermediate result data to the input data node of the single DES engine using the data select switch during a third DES processing operation;

selecting and coupling a third key from the key data to the key data node of the single DES engine using the key select switch during the third DES processing operation, the third key associated with the second intermediate result data;

third DES processing the second intermediate result data with the associated third key to obtain a third result from the third DES process operation; and

latching data from the third result to the DataOut bus of the security processing circuit.

26. The method of claim 25, further comprising transferring the data on the DataOut bus of the security processing circuit to the network interface device.

27. A method of performing 3DES cryptographic processing between a network and a host system using a security processing circuit employing a single DES engine within a network interface device to encrypt outgoing data from the host system to the network and to decrypt incoming data from the network to the host system, the method comprising:

latching input data to a DataIn bus of the network interface device, the input data associated with incoming data from the network during decryption, and associated with outgoing data from the host system during encryption;

latching key data to a Key bus of the network interface device;

selecting and coupling the input data to an input data node of the single DES engine using a data select switch during a first DES processing operation;

selecting and coupling a first key from the key data to a key data node of the single DES engine using a key select switch during the first DES processing operation, the first key associated with the input data;

first DES processing the input data with the associated first key using the single DES engine of the security processing circuit;

obtaining a first intermediate result data from the first DES processing operation at a DataOut bus of the security processing circuit, the intermediate result being feedback coupled to a feedback input of the data select switch;

selecting and coupling the intermediate result data to the input data node of the single DES engine using the data select switch during a second DES processing operation;

selecting and coupling a second key from the key data to the key data node of the single DES engine using the key select switch during the second DES processing operation, the second key associated with the intermediate result data;

second DES processing the intermediate result data with the associated second key;

obtaining a second intermediate result from the second DES processing operation at the DataOut bus of the security processing circuit, the second intermediate result being feedback coupled to the feedback input of the data select switch;

selecting and coupling the second intermediate result data to the input data node of the single DES engine using the data select switch during a third DES processing operation;

selecting and coupling a third key from the key data to the key data node of the single DES engine using the key select switch during the third DES processing operation, the third key associated with the second intermediate result data;

third DES processing the second intermediate result data with the associated third key to obtain a third result from the third DES process operation;

latching the third result data to the DataOut bus of the security processing circuit; and

transferring the output data on the DataOut bus of the security processing circuit to the network interface device, the output data associated with outgoing data from the host system to the network during encryption, and during decryption the output data associated with incoming data from the network to the host system.